REBECCA A. PETERSON (241858)
**GEORGE FELDMAN MCDONALD, PLLC**
1650 W. 82nd Street, Suite 880
Bloomington, MN 55431
Telephone: (612) 778-9595
E-mail: rpeterson@4-justice.com

**UNITED STATES DISTRICT COURT**

**EASTERN DISTRICT OF CALIFORNIA**

**SACRAMENTO DIVISION**

**DENISE CHAMPNEY,** *on behalf of herself,* **and NICOLE DRENNEN**, *on behalf of herself and as parent and guardian of her two minor children, John Doe and Jane Doe,* **and** *on behalf of all others similarly situated,*

Plaintiffs,

v.

**POWERSCHOOL HOLDINGS, INC.**,

Defendant.

**CLASS ACTION COMPLAINT FOR DAMAGES, INJUNCTIVE RELIEF, AND EQUITABLE RELIEF FOR:**

1. **Negligence**
2. **Breach of Fiduciary Duty**
3. **Invasion of Privacy**
4. **Declaratory Judgment**
5. **Unjust Enrichment**

**DEMAND FOR JURY TRIAL**

## CLASS ACTION COMPLAINT

1. Plaintiffs Denise Champney ("Champney"), on behalf of herself, and Nicole Drennen ("Drennen"), on behalf of herself and as parent and guardian of her two minor children, John Doe and Jane Doe (Plaintiffs Champney, Drennen, and Drennen's two minor children are collectively referred to as "Plaintiffs"), and on behalf of all other persons similarly situated, upon personal knowledge as to their experience, and upon information and belief as to all other matters, allege the following against PowerSchool Holdings, Inc. ("Defendant" or "PowerSchool"):

## NATURE OF THE ACTION

2. This Class Action Complaint is brought against Defendant to seek recovery by Plaintiffs and all other similarly situated people (the "Class" or "Class Members," defined herein), based upon Defendant's failure to properly secure and safeguard the personally identifiable

information ("PII") and personal health information ("PHI") (collectively, "Private Information") of PowerSchool users from cybercriminals.

3. Defendant PowerSchool operates an education technology ("EdTech") platform specializing in data collection, storage, and analytics. PowerSchool's primary customers are schools and school districts. In October 2024, PowerSchool was acquired by Bain Capital for $22.80 per share in cash, a total enterprise value of approximately $5.6 billion.[1]

4. PowerSchool serves over 60 million K-12 students in more than 90 countries.[2] Its products have been deployed in more than 90 of the largest 100 districts by student enrollment in the United States.

5. On December 28, 2024, PowerSchool learned that a hacker illegally accessed the Private Information of employees and students from customers worldwide by exploiting the user account of a PowerSchool technical support employee (the "Data Breach"). The cybersecurity hack resulted in the hacker gaining unauthorized access and downloading millions of records from schools worldwide from December 19, 2024 to December 24, 2024. Defendant did not detect the activity until December 28, 2024.

6. To date, PowerSchool has yet to disclose how many individuals have been affected by the Data Breach. PowerSchool is used in thousands school districts across the United States and, as such, there are likely millions of victims of this Data Breach.

7. The unauthorized actor accessed and/or downloaded students'–such as the minor children of Plaintiff Drennen (references to Plaintiff Drennen herein refer to Plaintiff Drennen and her two minor children)—Private Information, including upon information and belief, Social Security numbers and medical information, among other data points.[3]

8. For employees like Plaintiff Champney, the Private Information accessed and/or

---

[1] *Bain Capital Completes Acquisition of PowerSchool,* PowerSchool (Oct. 1, 2024), https://www.powerschool.com/bain-capital (last accessed Jan. 15, 2025).

[2] *Id.*

[3] *SIS Incident,* PowerSchool, https://www.powerschool.com/security/sis-incident/ (last accessed Jan. 15, 2025).

downloaded included, upon information and belief, Social Security numbers and medical information, ID numbers, their respective departments, employee type, school email addresses, and school phone numbers, among others.[4]

9. In order to utilize PowerSchool's services, students, students' parents, and the employees of Defendant's customers must provide Defendant with highly sensitive Private Information.

10. The data PowerSchool collects far exceeds traditional education records of school-aged children, including thousands of person-specific data fields.

11. PowerSchool does not fully disclose what data—or even categories of data—it collects from school-aged children, their parents, or school employees.

12. Due to the nature of the highly sensitive, confidential, and personal Private Information Defendant acquires, collects, maintains, and stores, Defendant had numerous statutory, regulatory, and common law duties to Plaintiffs and Class Members to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

13. Defendant disregarded the statutory, regulatory, and common law duties owed to Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt, accurate, and complete notice of the Data Breach.

14. Defendant was and remains required to maintain the security and privacy of the Private Information it took. When Plaintiffs and Class Members provided their Private Information to Defendant, Defendant was required to comply with the obligation to keep Plaintiffs' and Class Members' Private Information secure and safe from unauthorized access, to use this information for educational purposes only, and to make only authorized disclosures of this information.

[4] *Id.*

15. Plaintiffs' and Class Members' Private Information was accessed and/or downloaded by one or more unauthorized actors because Defendant failed to properly protect the Private Information of Plaintiffs and Class Members.

16. Armed with the Private Information accessed in the Data Breach, cybercriminals now have the means to commit a wide range of crimes, leaving Plaintiffs and the Class exposed to ongoing and imminent risk of various forms of identity theft. This threat will persist for the foreseeable future, and Plaintiffs and the Class will be forced to remain extra vigilant—constantly monitoring their financial accounts and personal data—due to Defendant's failures, in an attempt to prevent further victimization for the rest of their lives.

17. Mitigating that risk requires individuals to devote significant time, money and other resources to closely monitor their credit, financial accounts, health records and email accounts, as well as to take a number of additional prophylactic measures.

18. In this instance, all of that could have been avoided if Defendant had employed reasonable and appropriate data security measures.

19. Moreover, on information and belief, Defendant failed to mount any meaningful investigation into the breach itself, the causes, or what specific information of Plaintiffs and the proposed Class was lost to criminals.

20. To date, Defendant has yet to notify Plaintiffs of the Data Breach. Plaintiff Champney has only received notice of the Data Breach from her school district. Plaintiff Drennan also only received notice of the Data Breach from her minor children's school district.

21. Indeed, PowerSchool has refused to communicate directly with affected individuals, instead directing all communications to the "Technical Contacts in your organization who have received communication regarding the data breach."

22. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to

mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

23. Plaintiffs seek to remedy these harms on behalf of all similarly situated individuals whose private information was accessed and/or downloaded from Defendant's network during the Data Breach. Accordingly, Plaintiffs bring this class action lawsuit on behalf of themselves and on behalf of a class of individuals whose Private Information was accessed and/or downloaded by cybercriminals due to Defendant's negligent and reckless failures to implement reasonable and up-to-date cybersecurity measures to protect Plaintiffs and Class Members' sensitive Private Information.

## THE PARTIES

24. Plaintiff Champney is, and at all times relevant hereto has been, a citizen of the State of Rhode Island and resides in Washington County.

25. Plaintiff Champney is an employee of a school district in Rhode Island and was affected by the Data Breach.

26. Plaintiff Drennen is, and at all times relevant hereto has been, a citizen of the State of South Carolina and resides in Charleston County.

27. Plaintiff Drennan's two minor children attend school in a school district in Charleston County and are (and have been using) PowerSchool.

28. Defendant PowerSchool Holdings, Inc. is a citizen of the State of Delaware, with its principal place of business located at 150 Parkshore Dr., Folsom, California 95630. Defendant PowerSchool is an EdTech platform specializing in data collection, storage, and analytics, and serving schools and school districts.

## JURISDICTION & VENUE

29. This Court has subject matter and diversity jurisdiction over this action under 28

U.S.C. § 1332 of the Class Action Fairness Act of 2005 because this is a class action wherein (a) the amount in controversy exceeds $5,000,000, exclusive of interest and costs; (b) there are more than 100 members of the proposed class; and (c) there is minimal diversity because Plaintiffs (citizens of the States of Rhode Island and South Carolina) and Defendant are citizens of different states. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. § 1357.

30. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District. Further, Defendant is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of its business operations in this District, including decisions regarding the security of its customers' Private Information.

31. Venue is proper in this District under 28 U.S.C. § 1391(a)(1) through (d) because Defendant operates and maintains its principal place of business in this District and a substantial part of the events giving rise to this action occurred in this District.

## FACTUAL ALLEGATIONS

### A. Defendant Acquires, Collects, and Maintains, Plaintiffs' and Class Members' Private Information

32. Defendant PowerSchool is an EdTech platform specializing in data collection, storage, and analytics. Defendant offers software and technology-based solutions to schools and school districts. In providing its services, Defendant requires Plaintiffs and Class Members to provide their highly sensitive Private Information.

33. Defendant offers a product entitled PowerSchool Student Information System ("PowerSchool SIS").[5] PowerSchool SIS is a K-12 student information system designed to store and manage student data. The product is utilized by students, parents, and employees of schools and school districts.

34. Plaintiffs and Class Members are current and former students of Defendant's

[5] *PowerSchool SIS,* PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis (last accessed Jan. 13, 2025).

customers, students' parents, and employees of Defendant's customers.

35. In order to utilize Defendant's educational and/or employment services within the school setting, students, students' parents, and Defendant's customers' employees are required to provide Defendant with highly sensitive personal and health information.

36. For students and their parents, this Private Information included, upon information and belief, names, ID numbers, parent/guardian contact information, dates of enrollment and withdrawal reasons, medical alert information such as allergies and life-threatening conditions, disability information such as individualized education program ("IEP") and 504 plan status, Social Security numbers, and free and reduced lunch status (among others).

37. Defendant generates, collects, and retains Private Information without the effective consent of students and their parents.

38. For employees like Plaintiff Champney, the Private Information accessed and/or downloaded included, upon information and belief, names, Social Security numbers, medical information, ID numbers, their respective departments, employee type, school email addresses, and school phone numbers, among others.

39. Information relating to Plaintiff Champney's income, health insurance, retirement, and other employee benefit information may also have been affected by the Data Breach.

40. As part of Plaintiff Champney's official duties, she manages highly sensitive and confidential student information, including medical diagnoses, cognitive testing, and communications with medical professionals, all of which may have been affected by the Data Breach.

41. Plaintiff Drennen, her minor children, and Class Members live in states with compulsory education laws.

42. Plaintiff Drennen, her minor children, and Class Members live in a state that entitle residents to an education, which would include receiving and using services provided by their educational institutions, such as PowerSchool SIS.

43. Defendant made representations to its customers that they "place great importance and value on the proper handling of personal data that flows within [their] products as [they]

provide services to [their] customers."[6] It also claims that the PowerSchool SIS product is "secure by design" and that "your data is always protected with PowerSchool."[7]

44. Defendant further represents that they use "state-of-the-art, and appropriate physical, technical, and administrative security measures to protect the personal data that [they] process"[8] and that they do not "collect, maintain, use or share student personal information beyond that needed for authorized educational or school purposes, or as authorized by the parent or student."[9]

45. Plaintiffs and Class Members relied on Defendant's representations, either directly or indirectly through school administrators with whom they have a trusted relationship.

46. Students, their parents, and Defendant's customers' employees reasonably and appropriately expect that Defendant will safeguard their highly sensitive Private Information and keep it secure and confidential.

47. Plaintiff Drennan, her minor children, and similarly situated Class members maintain that they did not provide PowerSchool effective consent to generate, collect, process, store, or otherwise use their Private Information.

48. Even had all those affected by the Data Breach provided PowerSchool any such consent, due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its customers' students and employees, Defendant is required to keep customers' students' and employees' Private Information private; comply with industry standards related to data security and the maintenance of their customers' students' and employees' Private Information; inform their customers' students and employees of its legal duties relating to data security; comply with all federal and state laws protecting customers' students' and employees' Private Information; only use and release customers' students' and employees' Private Information

---

[6] *Privacy*, PowerSchool, https://www.powerschool.com/privacy/ (last accessed Jan. 15, 2025).

[7] *PowerSchool SIS,* PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last accessed Jan. 15, 2025).

[8] *Privacy*, PowerSchool, https://www.powerschool.com/privacy/ (last accessed Jan. 15, 2025).

[9] *Security,* PowerSchool, https://www.powerschool.com/security/ (last accessed Jan. 15, 2025).

for reasons that relate to the services it provides; and provide adequate notice to customers' students and employees if their Private Information is disclosed without authorization.

49. Defendant could not perform the services it provides without the required submission of Private Information from Plaintiffs and Class Members.

50. Plaintiffs and Class Members relied on Defendant, either directly or indirectly through school administrators, to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

51. Upon information and good-faith belief, Defendant's actions and inactions directly resulted in the Data Breach and the compromise of Plaintiffs' and Class Members' Private Information.

52. By generating, obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure. In other words, by generating, collecting and storing this Private Information, Defendant assumed an obligation to protect it.

53. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Defendant was required to keep Plaintiffs' and Class Members' Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

**B. The Data Breach**

54. On December 28, 2024, PowerSchool discovered that an unauthorized actor had gained access to and downloaded millions of records from schools worldwide by exploiting the user account of a PowerSchool technical support employee. This account allowed the unauthorized actor to gain unfettered access to the records between December 19, 2024 and December 24, 2024.

55. Plaintiff Champney received a Notice of Data Breach from the superintendent of her school district dated January 8, 2025, notifying her that her Private Information had been improperly exposed to unauthorized parties by Defendant (the "Champney Notice of Data

Breach").

56. Plaintiff Champney's Notice of Data Breach stated that her Private Information was accessed in the Data Breach, as follows in relevant part:

> I hope this message finds you well. I am writing to share important information about our student information system (SIS). PowerSchool, the company responsible for managing our SIS data, has notified us of a data breach. PowerSchool serves as the official platform for storing and managing information about students in XXXX, RI, and for millions of other students across the country. A copy of the notice from PowerSchool is attached.
>
> We understand this news may cause concern. While we are still gathering details about the breach, we have been informed that the incident was caused by administrative tools accessible only to PowerSchool. It is important to note that this situation was beyond the control of individual schools or the district.
>
> We are working with PowerSchool to assess this breach to its fullest extent and identify the necessary steps to safeguard our community's information. PowerSchool has shared that they will work with every district to provide proper communication per state statutes.
>
> Our students' and families' safety, privacy, and well-being remain our highest priorities. We are committed to transparency and will provide updates to all families and staff once we receive more information.

57. Plaintiff Champney's Notice of Data Breach message linked to the notice the district received from PowerSchool, as follows in relevant part:

> As the Technical Contact for your district or school, we are reaching out to inform you that on December 28, 2024, PowerSchool become aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed.
>
> Please review the following information and be sure to share this with relevant security individuals at your organization.
>
> As soon as we learned of the potential incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We have also informed law enforcement.
>
> We can confirm that the information accessed belongs to certain SIS customers and

> relates to families and educators, including those from your organization. The unauthorized access point was isolated to our PowerSource portal. As the PowerSource portal only permits access to the SIS database, we can confirm no other PowerSchool products were affected as a result of this incident.
>
> Importantly, the incident is contained, and we have no evidence of malware or continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor expects to experience, any operational disruption and continues to provide services as normal to our customers.
>
> Rest assured, we have taken all appropriate steps to prevent the data involved from further unauthorized access or misuse. We do not anticipate the data being shared or made public, and we believe it has been deleted without any further replication or dissemination.
>
> We have also deactivated the compromised credential and restricted all access to the affected portal. Lastly, we have conducted a full password reset and further tightened password and access control for all PowerSource customer support portal accounts.
>
> PowerSchool is committed to working diligently with customers to communicate with your educators, families, and other stakeholders. We are equipped to conduct a thorough notification process to all impacted individuals. Over the coming weeks, we ask for your patience and collaboration as we work through the details of this notification process.
>
> We have taken all appropriate steps to further prevent the exposure of information affected by this incident. While we are unaware of and do not expect any actual or attempted misuse of personal information or any financial harm to impacted individuals as a result of this incident, PowerSchool will be providing credit monitoring to affected adults and identity protection services to affected minors in accordance with regulatory and contractual obligations. The particular information compromised will vary by impacted customer. We anticipate that only a subset of impacted customers will have notification obligations.
>
> In the coming days, we will provide you with a communications package to support you in engaging with families, teachers and other stakeholders about this incident. The communications package will include tailored outreach emails, talking points, and a robust FAQ so that district and school leadership can confidently discuss this incident with your community.

58. Plaintiff Drennen also received a Notice of Data Breach from her minor children's school district, notifying her that her and her minor children's Private Information had been improperly exposed to unauthorized parties by Defendant between December 19, 2024 and December 24, 2024 (the "Drennen Notice of Data Breach").

59. Plaintiff Drennen further received an update on the Data Breach from her minor child's school district's Office of Communications on January 10, 2025, notifying her of the following:

- **Investigation Underway:** SCDE, SLED, and other state and federal agencies are actively investigating this incident.
- **Source of Breach:** The breach occurred through a compromised customer support credential belonging to PowerSchool.
- **PowerSchool's Response:** PowerSchool has taken full responsibility for the breach and has implemented measures to contain and mitigate the incident.

The SCDE has issued an official release with additional information, which you can access here.

60. The update Plaintiff Drennen received on January 8, 2025, linked to the notice the South Carolina Department of Education released, as follows in relevant part:

> Late Tuesday, the South Carolina Department of Education (SCDE) was informed by PowerSchool of a cybersecurity breach involving its PowerSource portal. This was an international incident over which the state and local districts had no control.
>
> This breach resulted in unauthorized access to certain customer data from PowerSchool's Student Information Systems (SIS), including data from multiple states and school districts across the country.
>
> During a meeting with PowerSchool's senior leadership, they confirmed that personally identifiable information (PII) was compromised. The SCDE is currently working to understand the full scope of the breach.
>
> PowerSchool has stated that this breach has been contained and has informed the SCDE that it has taken steps to secure its systems, engage cybersecurity experts, and is also coordinating with law enforcement to address the breach.
>
> The SCDE is actively communicating with PowerSchool, legal counsel, and local districts to assess the full impact on South Carolina schools, students, and educators and to determine next steps. The SCDE is also in direct communication with the State Law Enforcement Division (SLED), the Attorney General's office and has notified the Governor and legislative leaders.
>
> Commenting on the seriousness of this incident, State Superintendent of Education Ellen Weaver said, "The protection of our South Carolina students' and educators' personal data is non-negotiable. We fully recognize the anxiety this raises for them and their families."
>
> She continued, "While PowerSchool has taken accountability for this breach, our

> Department will take uncompromising action to ensure we uncover the complete extent of this incident. We will insist that PowerSchool not only notify affected individuals but also provide them with credit and identity monitoring services."

61. To date, PowerSchool has yet to disclose how many individuals have been affected by the Data Breach.

62. The unauthorized actor accessed and/or downloaded students' and students' parents' Private Information, including, upon information and belief, names, ID numbers, parent/guardian contact information, dates of enrollment and withdrawal reasons, medical alert information such as allergies and life-threatening conditions, disability information such as individualized education program ("IEP") and 504 plan status, Social Security numbers, and free and reduced lunch status.

63. For employees, the Private Information accessed and/or downloaded included, upon information and belief, names, Social Security numbers, medical information, ID numbers, their respective departments, employee type, school email addresses, and school phone numbers. Information relating to Plaintiff Champney's income, health insurance, retirement, and other employee benefit information may also have been affected by the Data Breach.

64. To date, Plaintiffs have yet to receive a notice of data breach directly from Defendant. The Notice of Data Breach Plaintiffs received from the school districts failed to provide basic details such as how the unauthorized actor accessed PowerSchool's networks, whether the data accessed was encrypted or otherwise protected, and how it learned of the Data Breach.

65. On information and belief, PowerSchool has refused to communicate directly with individuals whose Private Information has been compromised. On January 10, 2025, an individual potentially affected by the breach requested information from PowerSchool about the breach through its Community Forum website.[10] A PowerSchool moderator responded by recommending that the individual "work[] with the Technical Contacts in your organization who have received

[10] PowerSchool Community, Community Forum, https://help.powerschool.com/t5/Community-Forum/PowerSchool-Data-Breach/td-p/536290 (last accessed January 14, 2025).

communication regarding the data breach."[11] Another individual responded that they were the Technical Contact and that they "haven't received nearly enough information about the breach," including exactly which users and data were affected and information regarding monitoring services.[12]

66. The Data Breach occurred because Defendant did not implement adequate and reasonable cyber-security procedures and protocols to protect the Private Information of Plaintiffs and Class Members. Because Defendant's data security protocols and practices were deficient, unauthorized person(s) were able to access, view, and/or exfiltrate Plaintiffs' and Class Members' Private Information.

67. Defendant has reportedly engaged a third-party, cybersecurity firm to investigate the breach, requiring Plaintiffs and Class Members to wait another week for a final forensic report to reveal the true extent of the Data Breach.

68. To date, these omitted details have not been explained or clarified to Plaintiffs or Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

### C. Defendant Had Obligations to Protect Private Information under Federal and State Law and the Applicable Standards of Care

69. Defendant maintains and stores the Private Information of Plaintiffs and the Class in the usual course of business.

70. In generating, collecting, maintaining, and storing Private Information, Defendant promises to keep such information confidential and protect it from third parties. Defendant claims that it is "dedicated to protecting your students' data" and that its products are "independently validated by third-party auditors, ensuring your data is always protected with PowerSchool."[13]

71. Defendant also claims to have signed the national Student Privacy Pledge that

---

[11] *Id.*

[12] *Id.*

[13] *PowerSchool SIS,* PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last accessed Jan. 13, 2025).

states: "School service providers take responsibility to both support the effective use of student information and safeguard student privacy and information security."[14]

72. Under the Federal Trade Commission Act ("FTCA") (15 U.S.C. § 45), Defendant was prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has determined that a company's failure to implement reasonable and appropriate data security measures to protect consumers' sensitive personal information constitutes an "unfair practice" in violation of the Act. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

73. Under the Children's Online Privacy Protection Act ("COPPA") (16 C.F.R. § 312.8), Defendant was required to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children" under 13.

74. Defendant is also required by various state laws and regulations to protect Plaintiffs' and Class Members' Private Information.

75. In addition to its obligations under federal and state laws, Defendant had a duty to Plaintiffs and Class Members whose Private Information Defendant took. This duty required Defendant to exercise reasonable care in acquiring, retaining, securing, safeguarding, deleting, and protecting that information from compromise, loss, theft, unauthorized access, or misuse. Defendant owed Plaintiffs and Class Members an obligation to provide reasonable security measures, in line with industry standards and regulatory requirements, ensuring that its computer systems, networks, and personnel responsible for them adequately protected the Private Information of Plaintiffs and the Class Members from unauthorized exposure.

76. Defendant owed a duty to Plaintiffs and the Class Members, whose Private Information Defendant took, to design, maintain, and regularly test its computer and email systems to ensure that the Private Information in its possession was adequately secured and protected from unauthorized access or compromise.

77. Defendant owed a duty to Plaintiffs and the Class Members, whose Private

[14] *Security,* PowerSchool, https://www.powerschool.com/security/ (last accessed Jan. 13, 2025).

Information Defendant took, to establish and enforce reasonable data security practices and procedures to protect that information. This duty included properly training its employees and others with access to Private Information within its computer systems on how to securely handle and protect such data.

78. Defendant owed a duty to Plaintiffs and the Class Members, whose Private Information Defendant took, to maintain, update and otherwise ensure the security of PowerSchool SIS.

79. Defendant owed a duty to Plaintiffs and the Class Members, whose Private Information Defendant took, to implement processes capable of detecting, investigating and thwarting a breach in its data security systems in a timely manner.

80. Defendant owed a duty to Plaintiffs and the Class Members, whose Private Information Defendant took, to disclose if its computer systems and data security practices were inadequate to protect individuals' Private Information from theft. Such an inadequacy would constitute a material fact in the decision to provide personal information to Defendant.

81. Defendant owed a duty to Plaintiffs and the Class Members, whose Private Information Defendant took, to promptly and accurately disclose any data breaches that occurred.

82. Defendant owed a duty of care to Plaintiffs and the Class Members, as they were foreseeable and likely victims of any deficiencies in Defendant's data security practices.

**D. The Data Breach Was Foreseeable to Defendant and Preventable**

83. Despite the growing body of publicly available information regarding the rise of ransomware attacks and other forms of cyberattacks that compromise Private Information, Defendant's approach to maintaining the privacy of Plaintiffs' and Class Members' Private Information was inadequate, unreasonable, negligent, and reckless.

84. The Data Breach was clearly foreseeable to Defendant. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities.

85. Schools and school districts have been particularly and increasingly targeted by cybercriminals in recent years, which has resulted in leaks of highly personal and sensitive

information about children and educators, some of which perpetrators have made publicly available.

86. From 2016 to 2022, there were over 1,600 publicly disclosed cyberattacks on K-12 schools specifically, resulting in significant monetary losses to school districts ranging from $50,000 to $1 million per school data breach.[15]

87. The Data Breach was also clearly foreseeable to Defendant because Defendant was well aware that the Private Information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

88. Indeed, PowerSchool recently disclosed to shareholders that a "risk factor" was "the impact of potential information technology or data security breaches or other cyber-attacks or other disruptions[.]"[16] It admitted that "the techniques used by computer hackers and cyber criminals to obtain unauthorized access to data or to sabotage computer systems change frequently and generally are not detected until after an incident has occurred."[17]

89. Medical information, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.[18] Social Security numbers are among the most damaging types of Private Information to be stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change, as discussed below.

90. Furthermore, minor children are particularly vulnerable targets to identity theft because they are "often a blank slate for fraudsters who can apply for credit and take out loans in

---

[15] Juan H., *The biggest school data breaches of 2023,* Prey Project Blog (May 27, 2024) https://preyproject.com/blog/school-data-breaches-in-2023 (last accessed Jan. 15, 2025).

[16] Form 10-K, PowerSchool's 2023 United States Securities and Exchange Commission Report, https://s27.q4cdn.com/190453437/files/doc_financials/2023/q4/e46cee20-6b81-44d3-8885-dfccd31cd637.pdf (last accessed Jan. 15, 2025).

[17] *Id.*

[18] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (March 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed Jan. 15, 2025).

their name."[19] The risk to minors is substantial given their age and lack of established credit.

91. Such exposure can have immediate and long-term consequences for children. As explained by one cybersecurity professional whose son's school was hacked in an unrelated incident, "It's your future. It's getting into college, getting a job. It's everything."[20] And as PowerSchool itself has observed, such breaches can severely harm children in a variety of ways:

> could result in the loss or misuse of proprietary and confidential school, student (including prospective student), employee, and company information, or harm the safety, wellbeing, or academic outcomes of students, all of which could subject us to significant liability, or interrupt our business, potentially over an extended period of time. For example, data breaches or failures could result in a student's grades being misreported on that student's transcripts, which could negatively affect students' emotional health and educational and career prospects.[21]

92. 80. In 2022 alone, approximately 1.7 million minor children were victims of a data breach.[22]

93. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by the United States Government:

- **Implement an awareness and training program:** Educate employees and individuals about the threat of ransomware and how it is delivered, as end users are often the primary targets.
- **Enable strong spam filters:** Prevent phishing emails from reaching end users by using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to block email spoofing.

---

[19] *Are My Children at Risk of Identity Theft?,* Equifax, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/child-identity-theft (last accessed Jan. 15, 2025).

[20] Natasha Singer, *A Cyberattack Illuminates the Shaky State of Student Privacy*, The New York Times (July 31, 2022), https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html (last accessed Jan. 15, 2025).

[21] Form 10-K, PowerSchool's 2023 United States Securities and Exchange Commission Report, https://s27.q4cdn.com/190453437/files/doc_financials/2023/q4/e46cee20-6b81-44d3-8885-dfccd31cd637.pdf (last accessed Jan. 15, 2025).

[22] *Protecting Our Kids Data Privacy is Paramount,* Stay Safe Online (Jan. 25, 2024), https://www.staysafeonline.org/articles/protecting-our-kids-data-privacy-is-paramount (last visited Jan. 15, 2025).

- **Scan all incoming and outgoing emails:** Detect threats by scanning emails and filtering executable files to prevent them from reaching end users.

- **Configure firewalls:** Block access to known malicious IP addresses to prevent unauthorized access.

- **Patch operating systems, software, and firmware:** Regularly update and patch devices, potentially using a centralized patch management system for greater efficiency.

- **Set anti-virus and anti-malware programs for regular scans:** Ensure these programs run automatic scans to detect and remove potential threats.

- **Manage privileged accounts based on the principle of least privilege:** Limit administrative access to users only when absolutely necessary, and ensure those with admin privileges use them only when required. Implement an awareness and training program.

- **Configure access controls:** Implement least privilege principles for file, directory, and network share permissions. Users should only have access to what they need—if a user only needs to read specific files, they should not have write access to those files, directories, or shares.

- **Disable macro scripts in office files transmitted via email:** Prevent the execution of potentially harmful macros by disabling them in office files sent via email. Consider using Office Viewer software instead of full office suite applications to open email attachments.

- **Implement Software Restriction Policies (SRP):** Use SRPs or similar controls to prevent programs from executing from common ransomware locations, such as temporary folders associated with web browsers or compression programs, including the AppData/LocalAppData folder.

- **Disable Remote Desktop Protocol (RDP):** If RDP is not in use, consider disabling it to reduce potential attack vectors.

- **Use application whitelisting:** Allow only programs that are explicitly permitted by security policy to execute, blocking any unauthorized or potentially malicious software.

- **Execute operating system environments or specific programs in a virtualized environment:** Run sensitive systems or programs in isolated virtual environments to reduce risk.

- **Categorize data based on organizational value:** Implement physical and logical separation of networks and data for different organizational units to protect critical information and ensure appropriate access control.[23]

94. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by Microsoft's 2023 Digital Defense Report:

- **Enable multifactor authentication (MFA)**. This protects against compromised user passwords and helps to provide extra resilience for identifies.
- **Apply Zero Trust principles.** This includes ensuring users and devices are in a good state before allowing access to resources, allowing only the privilege that is needed for access to a resource and no more, assuming system defenses have been breached and systems may be compromised.
- **Use extended detection and response (XDR) and antimalware**. Implement software to detect and automatically block attacks and provide insights into the security operations software.
- **Keep up to date**. Unpatched out-of-date systems are a key reason many organizations fall victim to cyber-attacks.
- **Protect data**. Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.[24]

95. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by the FTC in its latest update to *Protecting Personal Information: A Guide for Business*:

- Know what personal information you have in your files and on your computers.
- Keep only what you need for your business.
- Protect the information that you keep.

---

[23] *How to Protect Your Networks from Ransomware: Technical Guidance Document,* United States Department of Justice, https://www.justice.gov/criminal/criminal-ccips/file/872771 (last accessed Jan. 15, 2025).

[24] *Microsoft Digital Defense Report 2023*, Microsoft https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023 (last accessed Jan. 15, 2025).

- Properly dispose of information you no longer need.
- Create a plan to respond to security incidents.[25]

96. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendant could and should have implemented the following preventive measures, as recommended by the Joint Ransomware Task Force's ("JRTF") #StopRansomware Guide, although this list does not encompass the full range of recommended actions:

- **Conduct regular vulnerability scanning to identify and address vulnerabilities**, especially those on internet-facing devices, to limit the attack surface.
- **Regularly patch and update software and operating systems to the latest available versions.** Prioritize timely patching of internet-facing servers-that operate software for processing internet data such as web browsers, browser plugins, and document readers-especially for known exploited vulnerabilities….
- **Limit the use of RDP and other remote desktop services.** If RDP is necessary, apply best practices. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later traverse the network using the native Windows RDP client.
- **Ensure all on-premises, cloud services, mobile, and personal devices are properly configured, and security features are enabled**. For example, disable ports and protocols that are not being used for business purposes.[26]

97. Given that Defendant took Private Information from Plaintiffs and the Class Members, Defendant should and could have taken the above measures to ensure that the Private Information generated and collected was safe from unauthorized actors.

98. The occurrence of the Data Breach indicates that Defendant failed to implement one or more of the above measures to prevent ransomware attacks. The failure to implement some or all of the above measures resulted in the Data Breach and the exposure of Plaintiffs' and Class

---

[25] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Jan. 15, 2025).

[26] *#StopRansomware Guide*, Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/resources-tools/resources/stopransomware-guide (last accessed Jan. 15, 2025).

Members' Private Information.

**E. Defendant Failed to Comply with FTC Guidelines**

99. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

100. For example, in 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines advise businesses, *inter alia,* to protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[27]

101. The guidelines further advise businesses: not to maintain PII longer than necessary for authorization of a transaction; to limit access to sensitive data; to use an intrusion detection system to expose a breach as soon as it occurs; to monitor all incoming traffic for activity indicating someone is attempting to hack the system; to watch for large amounts of data being transmitted from the system; and to verify that third-party service providers have implemented reasonable security measures.[28]

102. To underscore the binding significance and legal ramifications of the promulgated guidance, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.[29] Orders resulting from these actions

---

[27] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Jan. 15, 2025).

[28] *Id.*

[29] *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015) (determining that a company's failure to implement reasonable and appropriate data security measures to protect consumers' sensitive personal information constitutes an "unfair practice" in violation of the Act).

further clarify the measures businesses must take to meet their data security obligations.

103. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duties in this regard.

104. Defendant failed to properly implement basic data security practices, despite the amount, value, and sensitivity of the data it possessed.

105. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information, or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

106. Upon information and belief, Defendant was at all times fully aware of its obligations to protect the Private Information of Plaintiffs and Class Members, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it generated, obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

**F. Defendant Violated Industry Standards**

107. Experts studying cyber security routinely identify companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

108. In light of the evident threat of cyberattacks seeking Private Information from K-12 schools, several best practices have been identified by regulatory agencies and experts that, at a minimum, should be implemented by entities who are in possession of individuals' Private Information, including but not limited to: educating and training all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which

employees can access sensitive data; monitoring and limiting network ports; and protecting web browsers and email management systems. Defendant failed to follow these industry best practices, despite publicly acknowledging their importance.[30]

109. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

110. These foregoing frameworks are existing and applicable industry standards for large companies, and upon information and belief, Defendant failed to comply with these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

111. Moreover, the cybercriminal who accessed PowerSchool used an IP address from Ukraine.[31] Had PowerSchool taken the industry standard step of blocking non-US IP addresses from accessing U.S. instances, the Data Breach affecting Plaintiffs and Class Members could have been prevented.

**G. Plaintiffs' and Class Members' Private Information Has Significant Value**

112. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number,

---

[30] *Student Data Privacy: Everything You Need to Know*, PowerSchool (June 20, 2023) https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/ (last accessed Jan. 13, 2025).

[31] Lawrence Abrams, *PowerSchool hack exposes student, teacher data from K-12 districts,* Bleeping Computer (Jan. 7, 2025) https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/ (last accessed Jan. 15, 2025).

alien registration number, government passport number, employer or taxpayer identification number."[32]

113. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[33]

114. The Private Information of minor children is particularly valuable to criminals because they are "often a blank slate for fraudsters who can apply for credit and take out loans in their name."[34]

115. PowerSchool itself has observed that "the value of a student record on the black market is $250 to $350."[35]

116. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information at the point-of-sale in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

117. Take, for example, Social Security numbers, which are among the most damaging types of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration has stressed that the theft or loss of an individual's Social Security number, as occurred here, can lead to identity theft and extensive financial fraud:

---

[32] 17 C.F.R. § 248.201 (2013).

[33] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019) https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 15, 2025).

[34] *Are My Children at Risk of Identity Theft?*, Equifax, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/child-identity-theft (last accessed Jan. 15, 2025).

[35] *Student Data Privacy: Everything You Need to Know* PowerSchool (June 20, 2023) https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/ (last accessed Jan. 15, 2025).

> Identity theft is one of the fastest growing crimes in America. Scammers use your Social Security (SSN) to get other personal information about you. They can use your SSN and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your SSN until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.[36]

118. Moreover, the process of replacing a Social Security Number is time-consuming and difficult. According to the Social Security Administration, if your Social Security Number is lost or stolen, but there's no evidence of misuse, you cannot obtain a new number.[37] This leaves victims in a precarious situation, essentially forced to wait for fraud to occur before they can take action to mitigate the damage. This delay in being able to change a compromised Social Security Number puts victims at continued risk for identity theft, financial fraud, and other forms of exploitation, making it much harder to protect themselves in the aftermath of a data breach.

119. Among other forms of fraud, identity thieves may use Social Security Numbers to obtain driver's licenses, government benefits, medical services, and housing or even give false information to police. In addition, since teachers receive benefits and information regarding their benefits through their school email addresses, identify thieves could utilize information learned about a teacher to commit identity theft.

120. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a lag in time between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

---

[36] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 15, 2025).

[37] *Id.*

[38] *Report to Congressional Requesters,* GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed Jan. 15, 2025).

121. At all relevant times, Defendant knew or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, including Social Security Numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

122. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring, and will continue to incur, such damages in addition to any fraudulent use of their Private Information.

123. Defendant was, or should have been, fully aware of the unique types and the significant volume of data on its server(s) and thus the significant number of individuals who would be harmed by the compromised data.

124. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[39] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[40]

125. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be overstated. "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed[,] 69 percent reported feelings of fear related to personal financial safety[,] 60 percent reported anxiety[,] 42 percent reported fearing for

[39] *See Taking Charge, What To Do If Your Identity Is Stolen*, Federal Trade Commission, https://www.justice.gov/usao-wdmi/file/764151/dl?inline (last accessed Jan. 15, 2025).

[40] *See Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. §603.2(a). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 16 C.F.R. §603.2(b).

the financial security of family members[, and] 8 percent reported feeling suicidal."[41]

126. In addition to Social Security Numbers, unauthorized access to an individual's medical records can have serious consequences. Unlike credit or debit card information, which can be quickly replaced or canceled, stolen medical records can be stored for long periods, with individuals often remaining unaware that their records have been compromised or stolen.[42] Moreover, the monetary value of medical records on the dark web far exceeds that of credit card numbers. For example, the cybersecurity firm Trustwave discovered that medical records can fetch up to $250 per record on the dark web, while credit card numbers typically sell for around $5 each.[43]

127. Medical records are highly valuable to cybercriminals, not only because of the price for which they can be sold on the dark web, but also due to the various ways they can be exploited. Cybercriminals can use stolen medical records to commit medical identity theft to submit fraudulent medical claims, purchase prescriptions, or receive unauthorized treatment. These actions pose significant threats and risks to patients whose medical information has been compromised, leading to potential financial, physical, and emotional harm.

128. According to the FTC, if a hacker or an individual to whom the hacker sells your medical information mixes it with your own, it could impact the medical care you receive, or the health insurance benefits available to you. The FTC's Medical Identity Theft Frequently Asked Questions highlight several red flags victims should watch for, including: (i) receiving bills for medical services they didn't receive, (ii) being contacted by debt collectors about medical debt they don't owe, (iii) seeing unrecognized medical collection notices on their credit report, (iv) spotting incorrect office visits or treatments on their explanation of benefits, (v) being informed

---

[41] *Id.*

[42] *The Value of Protected Health Information (PHI) To Hackers: Understanding the Risks and Implications,* ifax, https://www.ifaxapp.com/hipaa/phi-hackers-risks-implications/ (last accessed Jan. 15, 2025).

[43] *Trustwave Global Security Report (2018)*, Trustwave, https://trustwave.azureedge.net/media/15350/2018-trustwave-global-security-report-prt.pdf?rnd=131992184400000000 (last accessed Jan. 15, 2025).

by their health plan that they've reached their benefits limit, or (vi) being denied insurance because their medical records reflect a condition they do not have.

129. These statistics highlight that the impact of identity theft extends far beyond financial harm—it profoundly affects individuals' physical well-being, mental health, and social relationships. This underscores just how critical it is to protect Private Information, as the consequences of its misuse ripple through every aspect of an affected person's life.

**H. Plaintiffs and Class Members Have Suffered Compensable Damages**

130. The ramifications of Defendant's failure to safeguard the Private Information of Plaintiffs and Class Members are long-lasting and severe. In 2023 alone, American adults lost $43 billion to identity theft.[44] Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

131. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information have diminished in value.

132. The Private Information belonging to Plaintiffs and Class Members is private in nature and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standard.

133. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

134. Defendant had the resources necessary to prevent the Data Breach—particularly

[44] *Identity Fraud Cost Americans $43 Billion in 2023,* AARP, https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html (last accessed Jan. 15, 2025).

after its recent $5.6 billion acquisition by Bain Capital—but neglected to adequately implement proper data security measures, despite its obligation to protect the Private Information.

135. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class Members' Private Information.

136. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

137. Defendant's failure to adequately protect Plaintiffs' and Class Members' Private Information has resulted in Plaintiffs and the Class Members having to undertake these tasks which require extensive amounts of time, calls and, for many of the credit and fraud protection services.

138. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at an increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Unauthorized use and misuse of their Private Information;

c. The loss of the opportunity to control how their Private Information is used;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of

criminals;

g. The continued risk to their Private Information that is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

i. Lost or diminished educational prospects and opportunities;

j. Lost or diminished career prospects and opportunities; and

k. Emotional distress resulting from the foregoing.

139. In addition to a remedy for economic harm, Plaintiffs and the Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

## REPRESENTATIVE PLAINTIFFS' EXPERIENCES

***Plaintiff Denise Champney***

140. Plaintiff Denise Champney is an employee of a Rhode Island school district that utilized PowerSchool SIS.

141. Plaintiff Champney was required to provide her Private Information to Defendant in order to utilize Defendant's services as an employee of one of Defendant's customers. Plaintiff Champney was required to provide her Private Information to Defendant in order to perform her employment related duties.

142. Information relating to Plaintiff Champney's income, health insurance, retirement, and other employee benefit information may also have been affected by the Data Breach.

143. Plaintiff Champney received a letter from her school district dated January 8, 2025, notifying her that her Private Information had been improperly exposed to unauthorized parties by Defendant.

144. Plaintiff emailed PowerSchool requesting additional information about the Data Breach and has not received a response.

145. Plaintiff is still awaiting formal and direct notice from Defendant detailing exactly how her Private Information has been compromised. Upon information and belief, her Social Security number and medical information, among other data points, were compromised.[45]

146. Because the Data Breach was an intentional attack by cybercriminals seeking valuable information that they could exploit, Plaintiff remains at critical risk of severe identity theft and exploitation.

147. Plaintiff is very careful about not sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

148. Plaintiff takes great care to store any documents containing her personal information in secure locations or to properly dispose of such documents. She also exercises caution by selecting unique usernames and strong passwords for her online accounts to protect her privacy and security.

149. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

150. Plaintiff will be taking steps to secure her Private Information and implementing

[45] *SIS Incident,* PowerSchool, https://www.powerschool.com/security/sis-incident/ (last accessed Jan. 15, 2025).

freezes on her credit with national credit reporting agencies.

151. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

152. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

153. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

154. Plaintiff has a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiff Nicole Drennen and her minor children***

155. Plaintiff Nicole Drennen is the parent and guardian of two minor children who are both students within a South Carolina school district that utilized PowerSchool SIS.

156. Plaintiff Drennen was required to provide her and her children's Private Information to Defendant in order to receive Defendant's services. Plaintiff Drennen was required to provide their Private Information to Defendant in order to attend school in their school district.

157. On January 6, 2025, before they were notified of the Data Breach, one of Plaintiff Drennen's children attempted to log into his Google Chromebook and was unable to because his password had been changed by an unauthorized actor.

158. Thereafter, Plaintiff Drennen received a letter from the superintendent of her school district, dated January 7, 2025, informing her that her and minor children's Private Information had been disclosed to an unauthorized actor as a result of the Data Breach.

159. Plaintiff Drennen is still awaiting formal and direct notice from Defendant detailing exactly how her and her children's Private Information has been compromised. Upon information and belief, this Private Information includes Social Security numbers and medical information,

among other data points.[46]

160. Because the Data Breach was an intentional attack by cybercriminals seeking valuable information that they could exploit, Plaintiff Drennen and her minor children remain at critical risk of severe identity theft and exploitation.

161. Plaintiff Drennen and her minor children are very careful about not sharing their sensitive Private Information. They have never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

162. Plaintiff Drennen and her minor children take great care to store any documents containing their personal information in secure locations or to properly dispose of such documents. They also exercise caution by selecting unique usernames and strong passwords for their online accounts to protect their privacy and security.

163. Plaintiff Drennen and her minor children suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

164. Plaintiff Drennen will be taking steps to secure her and her minor children's Private Information and implementing freezes on their credit with national credit reporting agencies.

165. The Data Breach has caused Plaintiff Drennen and her minor children to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence. This fear, anxiety, and stress has

[46] *Id.*

been further multiplied by Plaintiff's serious concern for her minor children and the impact on their credit and life—including their education and career prospects—before they have even reached adulthood.

166. As a result of the Data Breach, Plaintiff Drennen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach for her and her minor children.

167. As a result of the Data Breach, Plaintiff Drennen and her minor children are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

168. Plaintiff Drennen and her minor children have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

## CLASS ALLEGATIONS

169. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiffs seek to bring this class action on behalf of themselves, Plaintiff Drennen's minor children, and as members of the following classes against Defendant defined as follows:

> **All persons and/or entities in the United States whose Private Information was compromised in Defendant's Data Breach which occurred in or about December 2024 (the "Class").**
>
> **All students and students' parents in the United States whose Private Information was compromised in Defendant's Data breach which occurred in or about December 2024 (the "Students and Parents Subclass").**
>
> **All employees of Defendant's clients and/or customers in the United States whose Private Information was compromised in Defendant's Data breach which occurred in or about December 2024 (the "Employee Subclass").**

170. Excluded from the Class and Subclasses (collectively, "Classes") are Defendant and its officers, directors and employees, any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the Judges and Court personnel in this case and any members of their immediate

families.

171. Plaintiffs reserve the right to modify and/or amend the Classes, including but not limited to, creating additional subclasses as necessary.

172. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

173. ***Numerosity.*** Consistent with Fed. R. Civ. P. 23(a)(l), the Classes are so numerous that joinder of all members is impracticable. The exact size of the Class and the identities of Class Members are readily ascertainable in or through Defendant's records.

174. ***Commonality and Predominance.*** Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), this action involves common questions of law and fact that predominate over any questions that may affect only individual Class Members. Such common questions include:

a. Whether Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach;

b. Whether Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

c. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to further unauthorized third parties;

d. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members for non-education purposes;

e. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

f. Whether and when Defendant actually learned of the Data Breach;

g. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class Members' Private Information, and breached its duties thereby;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

i. Whether Defendant violated the law by failing to promptly notify Plaintiffs and

Class Members that their Private Information had been compromised;

j. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

k. Whether Defendant adequately addressed and fixed the vulnerabilities that allowed the Data Breach to occur;

l. Whether Defendant was negligent and that negligence resulted in the Data Breach;

m. Whether Defendant was unjustly enriched;

n. Whether Plaintiffs and Class Members are entitled to actual, statutory, and/or nominal damages as a result of Defendant's wrongful conduct; and

o. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

175. ***Typicality.*** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of the claims of other Class Members in that Plaintiffs, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiffs and all Class Members were injured through the misconduct of Defendant and assert the same claims for relief.

176. ***Adequacy.*** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs and their counsel will fairly and adequately protect the interests of the Classes. Plaintiffs are members of the Class they seek to represent; are committed to pursuing this matter against Defendant to obtain relief for the Classes; and have no interests that are antagonistic to, or in conflict with, the interests of other Class Members. Plaintiffs retained counsel who are competent and experienced in litigating class actions and complex litigation, including data breach litigation of this kind. Plaintiffs and their counsel intend to vigorously prosecute this case and will fairly and adequately protect the Classes' interests.

177. ***Superiority.*** Consistent with Fed. R. Civ. P. 23(6)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating

their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Classes. Plaintiffs and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

178. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3) because the common questions of law or fact predominate over any questions affecting Plaintiffs or any individual Class Members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

179. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(l) because the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. By contrast, conducting this litigation as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

180. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to Plaintiffs and the Classes as a whole, making injunctive and declaratory relief appropriate to Plaintiffs and the Classes as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retain possession of Plaintiffs' and Class Members' Private

Information, and has not been forced to change its practices or to relinquish Private Information by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Classes as a whole.

181. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present discrete common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. whether Plaintiffs' and Class Members' Private Information was accessed, compromised, or stolen in the Data Breach;

b. whether Defendant owed a legal duty to Plaintiffs and Class Members;

c. whether Defendant failed to take adequate and reasonable steps to safeguard the Private Information of Plaintiffs and Class Members;

d. whether Defendant failed to adequately monitor its data security systems;

e. whether Defendant failed to comply with applicable laws, regulations, and industry standards relating to data security;

f. whether Defendant knew or should have known that it did not employ adequate and reasonable measures to keep Plaintiffs' and Class Members' Private Information secure; and

g. whether Defendant's adherence to FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

## CAUSES OF ACTION

### COUNT I
### Negligence
### (On behalf of Plaintiffs & the Classes)

182. Plaintiffs repeat and re-allege and incorporate by reference herein all of the allegations above as if fully set forth herein.

183. Plaintiffs bring this claim individually and on behalf of the Classes.

184. Defendant owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in generating, obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

185. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

186. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By generating, collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

187. Defendant's duty also arose from Defendant's position as a provider of educational support services. Defendant holds itself out as trusted provider of educational support services, and thereby assumes a duty to reasonably protect Plaintiffs' and Class Members' information. Indeed, Defendant was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

188. Defendant breached the duties owed to Plaintiffs and Class Members and thus was negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiffs' and Class Members' Private Information, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Plaintiffs' and Class Members' information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a

reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to Plaintiffs and Class Members; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive Private Information.

189. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

190. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and/or imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information that Defendant took, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. Lost or diminished educational prospects and opportunities;

k. Lost or diminished career prospects and opportunities; and

l. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

191. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

**COUNT II**
**Breach of Fiduciary Duty**
**(On behalf of Plaintiffs & the Classes)**

192. Plaintiffs repeat and re-allege and incorporate by reference herein all of the allegations above as if fully set forth herein.

193. Plaintiffs bring this claim individually and on behalf of the Classes.

194. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs' and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

195. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—in particular to secure their Private Information.

196. Because of the highly sensitive nature of the Private Information, Plaintiffs and Class Members (or their third-party agents)—had they provided effective consent to Defendant taking their Private Information, which they did not—would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

197. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' Private Information.

198. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

199. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

## COUNT III
**Invasion of Privacy**
**(On behalf of Plaintiffs & the Classes)**

200. Plaintiffs repeat and re-allege and incorporate by reference herein all of the allegations above as if fully set forth herein.

201. Plaintiffs bring this claim individually and on behalf of the Classes.

202. Plaintiff and the Classes had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

203. Defendant owed a duty to its current and former users, including Plaintiffs and the Classes, to keep this information confidential.

204. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Private Information is highly offensive to a reasonable person.

205. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Classes (or their third-party agents) were required to disclose their sensitive and confidential information to Defendant, but did so privately, with the belief that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Classes were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

206. The Data Breach constitutes an intentional interference with Plaintiffs' and the Classes' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

207. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

208. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Classes in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

209. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Classes.

210. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Classes were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Classes to suffer damages (as detailed *supra*).

211. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Classes since their Private Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

212. Plaintiffs and the Classes have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Classes.

213. In addition to injunctive relief, Plaintiffs, on behalf of themselves, Plaintiff

Drennen's minor children, and the other Class members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

**COUNT IV**
**Declaratory Judgment and Injunctive Relief**
**(On behalf of Plaintiffs & the Classes)**

214. Plaintiffs repeat and re-allege and incorporate by reference herein all of the allegations above as if fully set forth herein.

215. Plaintiffs bring this claim individually and on behalf of the Classes.

216. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

217. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

218. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure users' Private Information and to timely notify users of a data breach under the common law, Section 5 of the FTC Act; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure students', parents' and employees' Private Information.

219. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect users' Private Information.

220. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant's properties.

221. The risk of another such breach is real, immediate and substantial.

222. If another breach of Defendant's store of student, parent, and employee data occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

223. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

224. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant's business, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

## COUNT V
## Unjust Enrichment
## (On behalf of Plaintiffs & the Classes)

225. Plaintiffs repeat and re-allege and incorporate by reference herein all of the allegations above as if fully set forth herein.

226. Plaintiffs bring this claim individually and on behalf of the Classes.

227. Upon information and belief, Defendant funded its data security measures from its general revenue including payments made by its customers for use by Plaintiffs, Plaintiff Drennen's minor children and Class Members, as well as by revenue generated from its data-sharing agreements, including data belonging to Plaintiffs, Plaintiff Drennen's minor children and Class Members.

228. As such, a portion of the payments made directly or indirectly on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

229. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their data to Defendant, including Private Information, which Defendant uses for highly profitable commercial purposes.

230. In exchange, Plaintiffs and Class Members received only education and/or employment services to which they were already legally entitled. This does not constitute adequate consideration for PowerSchool's taking of their Private Information.

231. Defendant knew that Plaintiffs and Class Members conferred a benefit that Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

232. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of data security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits and the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective data security measures.

233. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

234. Defendant failed to secure Plaintiffs and Class Members' Private Information and, for that and other reasons, did not provide full compensation for the benefit Plaintiffs and Class Members conferred upon Defendant.

235. Defendant acquired Plaintiffs' and Class Members' Private Information through unlawful means in that it generated and extracted such information without effective consent.

236. Defendant acquired Plaintiffs' and Class Members' Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

237. Plaintiffs and Class Members have no adequate remedy at law.

238. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of

the Data Breach for the remainder of the lives of Plaintiffs and Class Members;

j. Lost or diminished educational prospects and opportunities;

k. Lost or diminished career prospects and opportunities; and

l. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

239. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

240. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts overpaid, directly or indirectly on behalf of Plaintiffs and Class Members, for Defendant's services.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves, Plaintiff Drennen's two minor children, and other Class Members, pray for judgment against Defendant as follows:

A. That the Court certify this case as a class action and certify the Class as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

B. That Plaintiffs and the Classes be granted the declaratory and injunctive relief sought herein;

C. A judgment in favor of Plaintiffs and the Classes awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorneys' fees, expenses, costs, and such other and further relief as it just and proper in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

E. That the Court award pre- and post-judgment interest at the maximum legal rate; and

F. That the Court grant all such other relief as it deems just and proper.

**DEMAND FOR JURY TRIAL**

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff Champney, on behalf of herself, and Plaintiff Drennen, on behalf of herself and as parent and guardian of her two minor children, and on behalf of all others similarly situated and other members of the proposed Classes, hereby demand a jury trial of any and all issues so triable as of right.

Dated: January 15, 2025

Respectfully Submitted,

*/s/ Rebecca A. Peterson*
Rebecca A. Peterson (241858)
**GEORGE FELDMAN MCDONALD, PLLC**
1650 W. 82nd Street, Suite 880
Bloomington, MN 55431
Telephone: (612) 778-9530
rpeterson@4-justice.com
eservice@4-justice.com

Lori G. Feldman*
**GEORGE FELDMAN MCDONALD, PLLC**
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
lfeldman@4-justice.com
e-service@4-justice.com

Julie Liddell*
Andrew Liddell*
**EdTech Law Center**
P.O. Box 300488
Austin, Texas 78705
Telephone: (737) 351-5855
julie.liddell@edtech.law

Attorney for Plaintiffs and the Proposed Classes
*Pro hac vice forthcoming**